# Zur Haftung eines WLAN-Hotspot-Betreibers

## 1. Einleitung

Das Haftungssystem der Internet Service Provider (ISP) in Deutschland ist durch eine umfangreiche Rechtsprechung und den Einfluss der europäischen E-Commerce-RL sowie der deutschen Regelungen in Telekommunikationsgesetz (TKG) und Telemediengesetz (TMG) geprägt.

Bei der Bewertung der Haftung eines ISP sind insbesondere die Regelungen der §§ 7 ff. TMG zu beachten, die eine Haftungsprivilegierung von ISPs vorsieht. Das TMG unterscheidet zwischen verschiedenen ISPs: Dem Host Provider (§ 10 TMG), dem Cache Provider (§ 9 TMG) und dem Access Provider (§ 8 TMG). WLAN-Hotspots sind als Access Provider anzusehen, da sie den Zugang zu Information über eine Telekommunikations- bzw. einen Telekommunikationsdienst ermöglichen (allgemeine Auffassung, s. nur *Röhrborn/Katko*, CR 2002, 882; *Hoffmann*, in Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 8 Rn. 17; *Spindler*, CR 2010, 592, 595; *Mantz*, Rechtsfragen offener Netze, 2008, 48; jew. m.w.N.). Auf sie findet daher § 8 TMG Anwendung. Dieser lautet:

> ***§ 8 Durchleitung von Informationen***
> *(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie*
> *1. die Übermittlung nicht veranlasst,*
> *2. den Adressaten der übermittelten Informationen nicht ausgewählt und*
> *3. die übermittelten Informationen nicht ausgewählt oder verändert haben.*
> *Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.*
> *(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.*

## 2. Rechtsprechung

Die Rechtsprechung zur Haftung von ISPs ist vornehmlich an Fällen entwickelt worden, die Host Provider wie z.B. eBay betrafen. Zur Haftung des Betreibers eines öffentlichen WLAN-Hotspots liegt hingegen bisher praktisch keine Rechtsprechung vor. Die für Host Provider ergangene Rechtsprechung lässt sich allerdings nur eingeschränkt bis gar nicht auf den Betrieb eines WLAN-Hotspots übertragen (OLG Brandenburg, Beschl. v. 9.5.2012 – 13 U 50/10, MMR 2012, 625; ebenso die absolut h.M. in der Literatur s. *Spindler*, MMR 2008, 167, 168; *Zimmermann/Stender-Vorwachs*, in: Spindler/Schuster, Recht der elektronischen Medien, 1. Aufl. 2008, vor § 7 TMG Rn. 67; jew. m.w.N.). Nachfolgend soll daher ein kurzer Überblick über die hier relevante Rechtsprechung gegeben werden.

### a. Rechtsprechung zu WLAN-Hotspots

Bisher gibt es in der deutschen Rechtsprechung drei Entscheidungen, die sich explizit mit dem Betrieb eines öffentlichen WLAN-Hotspots befassen:

- LG Frankfurt, Urt. v. 18.8.2010 – 2-6 S 19/09, MMR 2011, 401: Keine Haftung eines Hotelinhabers, der ein WLAN betreibt, sein WLAN verschlüsselt und Gäste belehrt hat
- LG München, Urt. v. 12.1.2012 – 7 HK O 1398/11, CR 2012, 603: Keine Pflicht zur Identifizierung von Nutzern eines WLANs
- OLG Köln, Urt. v. 5.6.2009 – 6 U 223/08, MMR 2009, 695: Unlauterkeit des Geschäftsmodells von FON

Bereits die ersten beiden genannten Entscheidungen zeigen, dass ein Haftungsrisiko eher nicht besteht. Die Entscheidung des OLG Köln ist Entscheidung aus dem Bereich des Wettbewerbsrecht.

**b. Rechtsprechung zu privaten, nicht-öffentlichen WLANs**

Demgegenüber gibt es umfassende Rechtsprechung, die sich mit dem Betrieb eines privaten WLAN an einem privaten Internetanschluss befasst. Die Behandlung dieser Fälle war bis 2010 zwischen verschiedenen Gerichten umstritten. In seinem Urteil „Sommer unseres Lebens“ hat der BGH im Jahr 2010 (BGH, Urt. v. 12.5.2010 – I ZR 121/08, MMR 2010, 565) klargestellt, dass derjenige, der ein privates WLAN verschlüsselt betreibt einen ausreichend sicheren Schlüssel verwenden muss. Tut er dies nicht, kann er als Störer haften. Kennzeichnend für die Entscheidung ist, dass der BGH die Privilegierung des § 8 TMG (ohne nähere Begründung und gegen die einhellige Auffassung in der rechtswissenschaftlichen Literatur) auf den privaten Betreiber nicht angewendet hat.

Der Betrieb eines öffentlichen WLAN-Hotspots ist jedoch mit dem privaten Betrieb eines WLANs nicht zu vergleichen. Vielmehr ist die Privilegierung des § 8 TMG auf den Betreiber eines öffentlichen WLAN-Hotspots nach allgemeiner Auffassung anzuwenden. Daher dürfte die bisherige Rechtsprechung zu privaten WLANs, vorgehend und ausgehend von der Entscheidung „Sommer unseres Lebens“ auf den Betrieb eines öffentlichen WLAN-Hotspots praktisch nicht übertragbar sein.

**c. Rechtsprechung zur Haftung von Access Providern**

Vergleichbar ist aber die zur Haftung von Access Providern ergangene Rechtsprechung, nachfolgend eine Auswahl:

- OLG Frankfurt, Beschl. v. 22.1.2008 – 6 W 10/08, MMR 2008, 166: Access Provider ist für Informationen, zu denen er Zugang vermittelt, nicht verantwortlich
- OLG Karlsruhe, Urt. v. 8.5.2002 – 6 U 197/01, MMR 2002, 613: Access Provider haftet für Verletzung der Wettbewerbsordnung durch Kunden nicht
- LG Köln, Urt. v. 31.8.2011 – 28 O 362/10, MMR 2011, 833: Haftung des Access Providers würde Störerhaftung überdehnen
- LG Hamburg, Urt. v. 12.3.2010 – 308 O 640/08, MMR 2010, 488: Access Provider müssen nicht sperren oder filtern
- LG Kiel, Urt. v. 23.11.2007 - 14 O 125/07, MMR 2008, 123: Keine Haftung des Access Providers für vermittelte Inhalte
- LG Hamburg, Urt. v. 12.11.2008 – 308 O 548/08, MMR 2009, 506: Access Provider ist DNS-Sperre nicht zumutbar
- LG Düsseldorf, Urt. v. 12.12.2007 - 12 O 530/07, MMR 2008, 189: Access Provider unterliegt keinen Verkehrssicherungspflichten in Bezug auf vermittelte Inhalte

- LG Düsseldorf, Urt. v. 13.12.2007 - 12 O 550/07, MMR 2008, 349: Access Provider unterliegt keinen Verkehrssicherungspflichten in Bezug auf vermittelte Inhalte
- LG Frankfurt, Urt. Beschl. 5.12.2007 – 2-03 O 526/07, MMR 2008, 121: Access Provider unterliegt keinen Verkehrssicherungspflichten in Bezug auf vermittelte Inhalte
- VG Düsseldorf, Urt. v. 8.11.2011 – 27 K 5887/10: Access Provider ist nicht Störer
- VG Köln, Urt. v. 15.12.2011 – 6 K 5405/10, MMR 2012, 204: Access Provider ist nicht für Inhalte im Internet verantwortlich
- LG München I, Urt. v. 17.11.1999 – 20 Ns 465 Js 173158/95: Access Provider ist nicht strafbar, wenn er Zugang zu pornografischen Informationen im Internet ermöglicht (Compuserve)

Diese Aufzählung sollte zeigen, dass dem Access Provider nach den Grundsätzen der Störerhaftung Maßnahmen als Prüfungs- und Überwachungspflichten kaum auferlegt werden können. Gleiches dürfte auch im Hinblick auf die Haftung nach dem Modell der sog. Verkehrspflichten gelten, die im Übrigen auf den Access Provider keine Anwendung findet (OLG Frankfurt, Beschl. v. 22.1.2008 – 6 W 10/08, MMR 2008, 166 m. Anm. *Spindler*; *Spindler/Anton*, in Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 1004 BGB Rn. 10; *Döring*, WRP 2008, 1155, 1157).

### 3. Gesetzesänderung (?)

Durch die Rechtsprechung ist insbesondere für private Betreiber von WLANs eine gewisse Rechtsunsicherheit entstanden. Diese hat zu Reformbestrebungen auf der politischen Ebene geführt. So haben die SPD sowie Die LINKE jeweils Reformvorschläge bzw. –anregungen eingebracht. Diese sollten ausdrücklich klarstellen, dass § 8 TMG auf Unterlassungsansprüche und WLANs Anwendung finden soll (BT-Drs. 17/11145; BT-Drs. 17/11137; zu den Vorschlägen *Schmidt-Bens*, CR 2012, 828). Die Vorschläge sind in die entsprechenden Bundestagsausschüsse verwiesen worden (vgl. Plenarprotokoll 17/201 v. 25.10.2012, 24494 ff.). Am 13.5.2013 hat im Unterausschuss Neue Medien des Bundestages eine Anhörung zu dem Thema stattgefunden, in dem sich die Experten teilweise für eine Änderung der Regelungen zur Störerhaftung ausgesprochen haben. Dies haben sie u.a. damit begründet, dass die bisherige Rechtsprechung eine rechtswidrige Diskriminierung kleiner gewerblicher und privater WLAN-Betreiber darstelle. Ob der Gesetzesentwurf noch in dieser Legislaturperiode zu einer Abstimmung geführt wird, ist unklar. Ferner ist nicht klar, ob ggf. nach der kommenden Bundestagswahl erneut ein entsprechender Gesetzesentwurf eingebracht werden wird.

### 4. Pflicht zur Identifizierung der Nutzer

Teilweise wird im Hinblick auf den Betrieb eines WLANs gefragt, ob es eine Verletzung der Prüfungs- und Überwachungspflichten (im Rahmen der Störerhaftung) darstellt, wenn der Betreiber eines WLAN-Hotspots seine Nutzer nicht vor der Gewährung des Zugangs identifiziert, ob also eine Identifizierungspflicht besteht. Als Hintergrund wird z.B. angeführt, dass auf diese Weise das Haftungsrisiko im Rahmen der Störerhaftung ausgeschlossen bzw. reduziert werden könne.

Im Hinblick auf WLANs ist eine solche Pflicht in der Rechtsprechung bisher nicht bejaht worden. Für einen Forenbetreiber hat das OLG Düsseldorf im Jahr 2006 eine solche Pflicht zur Erhebung von Nutzerdaten angenommen (OLG Düsseldorf, Urt. v. 26.4.2006 – I-15 U

180/05, MMR 2006, 553), das LG Leipzig im Jahr 2004 für einen Anbieter von Subdomains (LG Leipzig, Urt. v. 13.11.2003 – 12 S 2595/03, MMR 2004, 263).

Diese Rechtsprechung dürfte zum einen nicht auf den Betreiber eines WLAN-Hotspots übertragbar sein, zum anderen sind die Entscheidungen durch aktuelle Entscheidungen (u.a. des OLG Düsseldorf) überholt (a.). Eine Identifizierungspflicht dürfte weiter für den Betreiber eines WLAN-Hotspots eine unzumutbare Maßnahme darstellen (b.), die ohne entspreche weitere Rechtfertigung z.B. durch Einwilligung des Nutzers gegen geltendes Datenschutzrecht verstoßen dürfte (c.).

**a. Keine Übertragbarkeit der Entscheidungen, aktueller Stand der Rechtsprechung**

Die Entscheidung des OLG Düsseldorf bezieht sich ausdrücklich auf den Betrieb eines Forums. Was für Forenbetreiber als Host Provider gilt, ist auf Access Provider allerdings nicht übertragbar (OLG Brandenburg, Beschl. v. 9.5.2012 – 13 U 50/10, MMR 2012, 625). Das LG Leipzig wiederum hat sich für den Subdomain-Anbieter maßgeblich auf die Praxis der DeNIC berufen, die eine Identifizierung durchführt bzw. durchführen lässt. Dies dürfte für Access Provider jedoch gerade nicht automatisch gelten.

Im Gegensatz dazu erkennen die Gerichte mittlerweile in aktuellen Entscheidungen an, dass eine Pflicht zur Identifizierung gerade nicht besteht. Das LG München I hat sich konkret im Hinblick auf den Betrieb eines WLAN-Hotspots mit allen denkbaren Normen beschäftigt, die eine Identifizierungspflicht begründen könnten und diese ausdrücklich abgelehnt (LG München I, Urt. v. 12.1.2012 - 7 HK O 1398/11, CR 2012, 605). Auch im Hinblick auf Verkehrsdaten erkennen die Gerichte an, dass eine Pflicht zur Erhebung und Speicherung gerade nicht besteht, selbst wenn dadurch eine spätere Auskunft an den Geschädigten nicht mehr möglich sein sollte. Eine solche Pflicht lässt sich insbesondere nicht aus den Grundsätzen der Störerhaftung ableiten (zuletzt OLG Düsseldorf, Beschl. v. 7.3.2013 – I-20 W 121/12, K&R 2013, 344 m. Anm. *Mantz* m.w.N.). Der EuGH hat eine solche Pflicht nicht per se als unzulässig angesehen (EuGH, Urt. v. 12.7.2011 – C 324/09, GRUR 2011, 1025 Rn. 142 – L'Oreal vs. eBay m. krit. Anm. *Hoeren*; dazu *Spindler*, MMR 2011, 703, 706), erforderlich wäre dafür aber nach der dargestellten Rechtsprechung eine entsprechende gesetzliche Regelung.

Zusätzlich haben das LG Frankfurt (Beschl. v. 4.10.2012 - 2-3 O 152/12, MMR 2013, 56) und das LG München I (Urt. v. 22.3.2013 – 21 S 28809/11, erscheint demnächst in MMR 6/2013) auch für den privaten Anschlussinhaber klargestellt, dass er – soweit er seiner sekundären Darlegungslast nachzukommen vermag - nicht als Störer haftet, selbst wenn er den eigentlichen „Täter" nicht benennt. Hierzu ist er prozessual nicht verpflichtet.

**b. Unzumutbarkeit einer Identifizierung**

Die einem Betreiber von WLAN-Hotspots auferlegte Pflicht zur Identifizierung der Nutzer im Rahmen der Bereitstellung eines (auch zeitweise) kostenlosen WLAN-Hotspots dürfte hingegen unzumutbar sein.

Die Pflicht zur Identifizierung würde ein erhebliches Hindernis beim Betrieb eines kostenlosen WLAN-Hotspots darstellen. Denn es kann zum einen davon ausgegangen werden, dass viele Nutzer sich von einer Identifizierung abschrecken lassen werden. Zusätzlich müsste – um die angeblich notwendige Maßnahme auch effektiv zu gestalten – eine Authentifizierung stattfinden, beispielsweise über das kostenintensive und langwierige Post-Ident. Ausländische Nutzer könnten dadurch von vornherein ausgeschlossen sein.

Hinzu käme, dass die Identifizierungspflicht datenschutzrechtliche Probleme aufwirft, die ebenfalls für eine Unzumutbarkeit sprechen (s. sogleich). Denn eine Pflicht, die den Anbieter zu einem rechtswidrigen Verhalten zwingen würde, ist per se unzumutbar.

**c. Datenschutzrechtliche Aspekte einer Identifizierungspflicht**

Jede Erhebung, Speicherung und Nutzung von Daten ist nach dem Grundsatz des Verbots mit Erlaubnisvorbehalt gemäß § 4 Abs. 1 BDSG nur gestattet, wenn sie durch Gesetz oder Einwilligung gerechtfertigt ist. Besteht eine Rechtfertigung, ist nach dem Zweckbindungsprinzip die Datenverwendung beschränkt auf den konkret gerechtfertigten Zweck. Bei Verträgen, die eine entgeltpflichtige Leistung betreffen, wird in der Regel von einer Rechtfertigung über § 28 Abs. 1 BDSG ausgegangen, da die Erhebung, Speicherung und Nutzung der Daten für die Abwicklung der Abrechnung erforderlich ist. Dabei ist allerdings zu beachten, dass § 13 Abs. 6 TMG bei Telemediendiensten sogar ausdrücklich die anonyme Bezahlung vorsieht und verlangt.

Bei kostenlosen Dienstleistungen, wie dem Angebot eines kostenlosen WLAN, besteht für eine Abrechnung grundsätzlich kein Erfordernis. Dementsprechend wäre eine Erhebung – ohne andere Rechtfertigung – grundsätzlich rechtswidrig.

Die Datenerhebung kann auch nicht durch das abstrakte Argument der Erforderlichkeit für eine spätere Beauskunftung gerechtfertigt werden. Die Gerichte haben immer wieder klargestellt: Ein Auskunftsanspruch beinhaltet weder eine Pflicht, noch ein Recht zur Erhebung und Speicherung (OLG Düsseldorf, Beschl. v. 7.3.2013 – I-20 W121/12, K&R 2013, 344 m. Anm. *Mantz* m.w.N.). Dies gilt erst recht für die Störerhaftung, die aus § 1004 BGB abgeleitet bzw. auf die entsprechenden Spezialnormen, z.B. § 97 Abs. 1 UrhG gestützt wird. Würde man auf Basis einer möglichen Haftung (z.B. nach den Grundsätzen der Störerhaftung) eine Erhebung und Speicherung von Daten rechtfertigen, würde dies § 4 Abs. 1 BDSG vollständig aushebeln, da jede Datenerhebung mit der potentiellen Pflicht zur Auskunft gerechtfertigt werden könnte.

Eine Rechtfertigung wäre daher allenfalls durch die Einholung der Einwilligung der Nutzer zu rechtfertigen. Diese müsste dann z.B. über die Portalseite eingeholt werden und den entsprechenden Anforderungen des § 4a BDSG sowie den Vorgaben des TMG entsprechen. Soweit die Daten für andere Zwecke erhoben und genutzt werden sollen (z.B. Werbung) sind die entsprechenden Einwilligungserklärungen entsprechend zu gestalten (s. nur zuletzt zur Unwirksamkeit der Datenschutz-Klauseln von Apple LG Berlin, Urt. v. 30.4.2013 – 15 O 92/12).